RETURN BID TO/ RETOURNER LES SOUMISSIONS À :

receptionsoumission-bidsreceiving.spp@international.gc.ca

Department of Foreign Affairs, Trade and Development (DFATD)
Ministère des Affaires étrangères, Commerce et Développement (MAECD)

Request for Proposal
Demande de proposition

Proposal to:
Department of Foreign Affairs, Trade and Development
We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached here to, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefore.

Proposition à:
Ministère des Affaires Étrangères, Commerce et Développement
Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux appendices ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments — Commentaires :

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT — LE PRÉSENT DOCUMENT COMPORTE UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ

Issuing Office – Bureau de distribution

Foreign Affairs, Trade and Development Canada
200 Promenade du Portage,
Gatineau, Québec, K1A 0G4

Affaires étrangère, Commerce et Développement Canada
200 Promenade du Portage,
Gatineau, Québec, K1A 0G4

Title-Sujet: Hosted Web Based Application Solution (HWBA)

Sollicitation No. — Nº de l'invitation 20-160060	**Date:** NOVEMBER 12, 2020
Sollicitation Closes — L'invitation prend fin	**Time Zone —Fuseau horaire**
At /à: **2 :00 PM** On / le **DECEMBER 23, 2020**	EDT(Eastern Daylight Time) / HAE (heure avancée de l'Est)

F.O.B. — F.A.B.
Plant-Usine: ☐ **Destination: X** **Other — Autre:** ☐

Address Enquiries to — Addresser les questions à:

Name: Houssam Hannat

Email: Houssam.Hannat@international.gc.ca

Telephone No. – No de téléphone:

(343) 203-5473

Destination of Goods and or Services/ Destination – des biens et ou services :

Department of Foreign Affairs, Trade and Development (DFATD) / Ministère des Affaires étrangères, Commerce et Développement (MAECD)

Vendor/Firm Name and Address — Nom du Vendeur et adresse du fournisseur/de l'entrepreneur:

Telephone No. – No de téléphone:

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) — Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

_____
Name, Title

_____ _____
Signature Date

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Work, the Basis of Payment, the Security Requirements Checklist, The Evaluation Criteria, and the Federal Contractors Program for Employment Equity - Certification,

1.2 Summary

1.2.1

a. The Department of Foreign Affairs, Trade and Development (DFATD) has requirement for a Hosted Web Based Application Solution (HWBA) for the Europe, Middle East and African, the United States, the Asia Pacific and the Americas regions, consisting of ± 178 geographic locations who will require access but who will be serviced through seven (7) Common Service Delivery Points (CSDP). The department requires an HWBA solution to manage a high volume of applicants for advertised vacancies in various locations across the world. The system must be an all-encompassing HR hiring platform designed to incorporate every hiring steps from posting vacancies, sourcing candidates to managing resume, administering exams, allowing online interviews and reference verification. With CSDP Human Resources (HR) teams directing and coordinating all of the recruitment activity in the various locations, a new and improved system is required.

b. It is intended to award of one (1) contract for three (3) years, plus four (4) one (1) year irrevocable option periods allowing Canada to extend the term of the contract.

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

1.2.3 The Federal Contractors Program (FCP) for employment equity applies to this procurement; refer to Part 5 – Certifications and Additional Information, Part 7 - Resulting Contract Clauses and the annex titled Federal Contractors Program for Employment Equity - Certification.

1.2.4 The requirement is subject to the provisions of the following trade agreement(s):

- Canadian Free Trade Agreement (CFTA)
- Canada-Chile Free Trade Agreement (CCFTA)
- Canada-Colombia Free Trade Agreement (CColFTA)
- Canada-Honduras Free Trade Agreement (CHFTA)
- Canada-Panama Free trade Agreement (CPanFTA)
- Canada-Peru Free Trade Agreement (CPFTA)
- Canada-Korea Free Trade Agreement (CKFTA)
- Canada-European Union Comprehensive Economic and Trade Agreement (CETA);
- World Trade Organization Agreement on Government Procurement (WTO-AGP)

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2020-05-28) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 120 days

2.1.1 *SACC* Manual Clauses

The following Supplemental General conditions are incorporated by reference and apply to and form part of the Contract:

i. 4003 (2010-08-16), Supplemental General Conditions - Licensed Software.

ii. 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software.

2.2 Submission of Bids

Bids must be submitted only to Department of Foreign Affairs and Trade Canada (DFATD) Bid Receiving Unit email address by the date, time and place indicated on page 1 of the Request for Proposal.

Due to the nature of the bid solicitation, bids transmitted by facsimile to DFATD will not be accepted.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump-sum payment must bear the closest public scrutiny and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPS, bidders must provide in writing before contract award for each question below, the answer and, as applicable, the information required.

If the Contracting Authority has not received the answer to the question and, as applicable, the information required by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the answer and, as applicable, the information required. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause,

"former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the

Royal Canadian Mounted Police. A former public servant may be:

(a) an individual;
(b) an individual who has incorporated;
(c) a partnership made of former public servants; or
(d) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act (PSSA)*, R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, *the Members of Parliament Retiring Allowances Act*, R.S., 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension?

Yes ( ) No ( )

If so, the Bidder must provide the following information for all FPS in receipt of a pension, as applicable:

(a) name of former public servant; and
(b) date of termination of employment or retirement from the Public Service.

By providing this information, bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive?

Yes ( ) No ( )

If so, the Bidder must provide the following information:

a) name of former public servant;
b) conditions of the lump sum payment incentive;
c) date of termination of employment;
d) amount of lump-sum payment;
e) rate of pay on which lump sum payment is based;
f) period of lump-sum payment including start date, end date and number of weeks; and
g) number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than seven (7) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.6 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least seven (7) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Bid Challenge and Recourse Mechanisms

(a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

(b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

- Office of the Procurement Ombudsman (OPO)
- Canadian International Trade Tribunal (CITT)

(c) Suppliers should note that there are **strict deadlines** for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Canada requests that bidders provide their bid in separately bound sections as follows:

Section I: Technical Bid (one (1) electronic copy)
Section II: Financial Bid (one (1) electronic copy)
Section III: Certifications (one (1) electronic copy)

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

Canada requests that bidders follow the format instructions described below in the preparation of their bid

a. use a numbering system that corresponds to the bid solicitation;
b. include a title page at the front of each section of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative.

Submission of Only One Bid:

i. A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will provide those Bidders with two (2) working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified.

ii. For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity is a natural person, corporation, partnership, etc.), an entity will be considered to be "related" to a Bidder if:

A. they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

B. they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act*;

C. the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

D. the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

iii. Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture.

a. **Joint Venture Experience**:

i. Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

ii. A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder has 3 years of experience providing maintenance service, and (b) that the bidder has 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

iii. Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint

venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submit this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

iv. Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

The technical bid consists of the following:

i. **Bid Submission Form**: Bidders are requested to include the Bid Submission Form – Attachment “3.1” with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name, the Bidder’s Procurement Business Number, the Bidder’s status under the Federal Contractors Program for Employment Equity, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.

ii. **Substantiation of Technical Compliance**:
The technical bid must substantiate the compliance of the bidder and its products and services with the specific requirements of **Attachment 1 to Part 4**, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition

of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or product complies is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of **Attachment 1 to Part 4**, where Bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

iii. **For Previous Similar Projects:** Where the bid must include a description of previous similar projects: (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder); (ii) a project must have been completed by the bid closing date; (iii) each project description must include, at minimum, the name and either the telephone number or e-mail address of a customer reference; and (iv) if more similar projects are provided than requested, Canada will decide in its discretion which projects will be evaluated. A project will be considered "similar" to the Work to be performed under any resulting contract if the project was for the performance of work that closely matches the *descriptions [or* of the Resource Categories identified in Annex A. Work will be considered to "closely match" if the work in the provided project is described in at least 50% of the points of responsibility listed in the description of the given Resource Category.

iv. **For Proposed Resources**: The technical bid must include résumés for the resources as identified in Attachment 1 to Part 4.

The Technical bid must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:

A. Proposed resources may be employees of the Bidder or employees of a subcontractor, or these individuals may be independent contractors to whom the Bidder would subcontract a portion of the Work

B. For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource by the time of bid closing. If the degree, designation or certification was issued by an educational institution outside of Canada, the Bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

C. For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of bid closing and must continue, where applicable, to be a member in good standing of the profession or membership throughout the evaluation period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this solicitation. If the entity is not specified, the issuer must be an accredited or otherwise recognized body, institution or entity at the time the document was issued. If

the degree, diploma or certification was issued by an educational institution outside of Canada, the Bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

D. For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal cooperative programme at a post-secondary institution.

E. For any requirements that specify a particular time period (e.g., 2 years) of work experience, Canada will disregard any information about experience if the technical bid does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.

F. For work experience to be considered by Canada, the technical bid must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

v. **Customer Reference Contact Information**:

A. In conducting its evaluation of the bids, Canada may, but will have no obligation to request that a bidder provide customer references. If Canada sends such a written request, the bidder will have 2 working days to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive. These customer references must each confirm if requested by Canada, the facts identified in the Bidder's bid, as required by Attachment 1 to part 4.

B. The form of question to be used to request confirmation from customer references is as follows:

"Has [the Bidder] provided your organization with [describe the services and, if applicable, describe any required time frame within which those services must have been provided]?"

___ *Yes, the Bidder has provided my organization with the services described above.*

___ *No, the Bidder has not provided my organization with the services described above.*

___ *I am unwilling or unable to provide any information about the services described above.*

C. For each customer reference, the Bidder must, at a minimum, provide the name, the telephone number and e-mail address for a contact person. Bidders are also requested to include the title of the contact person. If there is a conflict between the information provided by the customer reference and the bid, the information provided by the customer reference will be evaluated instead of the information

in the bid. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.

Section II: Financial Bid

A. Bidders must submit their financial bid in Canadian funds and in accordance with the Basis of selection detailed in Annex "B".

B. Bidders must submit their price and rates; Canadian customs duties and excise taxes included, as applicable; and Applicable Taxes excluded.

C. When preparing their financial bid, Bidders should review clause 4.2, Financial Evaluation, and article 7.7, Payment, of Part 7 of the bid solicitation.

D. Electronic Payment of Invoices - Bid

The Bidder accepts to be paid by the following Electronic Payment Instrument(s):

- Direct Deposit

Section III: Certifications

Bidders must submit the certifications and additional information required under Part 5.

3.1.2 Bidder's Proposed Sites or Premises Requiring Safeguarding Measures

3.1.2.1 As indicated in Part 6 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals' sites or premises for which safeguarding measures are required for Work Performance:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

3.1.2.2 The Company Security Officer must ensure through the Contract Security Program that the Bidder and proposed individuals hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical evaluation criteria.

An evaluation team composed of representatives of Canada will evaluate the bids.

The consensus evaluation team will consist of two (2) teams. One team will be responsible for the evaluation of the Business Requirements. The other team consisted of IM/IT Security experts will solely be responsible for the evaluation of the Security Requirements.

4.1 Technical Evaluation

4.1.1 Mandatory Technical Criteria

Refer to Attachment 1 of Part 4.

4.1.2 Point Rated Technical Criteria

Refer to Attachment 1 of Part 4.

4.2 Financial Evaluation

Bidders must submit their financial bid in Canadian dollars, in accordance with the Basis of payment at Annex "B". The price of the bid for financial evaluation purpose is the sum of: **the initial contract period cost + all option periods cost**, Applicable Taxes excluded, FOB destination, Canadian customs duties and excise taxes included.

4.3 Basis of Selection

4.3.1 Basis of Selection – Highest Combined Rating of Technical Merit 70% and Price 30%

1. To be declared responsive, a bid must:

    a. comply with all the requirements of the bid solicitation;
    b. meet all the mandatory evaluation criteria; and
    c. obtain the required minimum number of points specified in Attachment 1 to Part 4 for the point rated technical criteria.

2. Bids not meeting (a) or (b) or (c) will be declared non-responsive.

3. The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70% for the technical merit and 30% for the price.

4. To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70%.

5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30%.

6. For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

7. Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of the technical merit and price, respectively. The total available points equal 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)

		Bidder 1	Bidder 2	Bidder 3
Overall Technical Score		115/135	89/135	92/135
Bid Evaluated Price		$55,000.00**	$50,000.00**	$45,000.00*
Calculations	**Technical Merit Score**	115/135*** x 70 = 59.63	89/135*** x 70 = 46.15	92/135*** x 70 = 47.70
	Pricing Score	45/55 x 30 = 24.55	45/50 x 30 = 27.00	45/45 x 30 = 30.00
Combined Rating		84.18	73.15	77.70
Overall Rating		**1st**	**3rd**	**2nd**

In the example above, Bidder 1 would be recommended for contract award.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the procurement process.

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.2 Federal Contractors Program for Employment Equity - Bid Certification (Refer to Attachment 1 to Part 5)

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's website (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#).

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid list at the time of contract award.

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed annex titled Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements

1. At the date of bid closing, the following conditions must be met:

   (a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

   (b) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

   (c) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;

   (d) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

   (e) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.

2. For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work in Annex "A".

7.2 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

7.2.1 General Conditions

2035 (2020-05-28), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

7.2.2 Supplemental General Conditions

The following Supplemental General conditions are incorporated by reference and apply to and form part of the Contract:

i. 4003 (2010-08-16), Supplemental General Conditions - Licensed Software.

ii. 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software.

7.3 Security Requirements

7.3.1 The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Contract.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:
PWGSC FILE No. 20-160060

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED A, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

3. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CSP, PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED.

4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

5. The Contractor/Offeror must comply with the provisions of the:

(a) Security Requirements Check List and security guide (if applicable), attached at Annex C;
(b) Industrial Security Manual (Latest Edition)

7.3.2 Contractor's Sites or Premises Requiring Safeguarding Measures

7.3.2.1 Where safeguarding measures are required in the performance of the Work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individuals' sites or premises for the following addresses:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

7.3.2.2 The Company Security Officer must ensure through the Contract Security Program that the Contractor and individuals hold a valid security clearance at the required level.

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is from January 11th, 2021 to January 10th, 2024.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to four (4) additional one (1) year periods under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment at Annex "B".

Canada may exercise options at any time by sending a written notice to the Contractor at least 15 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is:

Name: Houssam Hannat
Title: Procurement Specialist
Department: Department of Foreign Affairs, Trade and Development
Address: 200 Promenade du Portage, Gatineau, Québec Canada K1A 0G4
Telephone: 343-203-5473
E-mail address: houssam.hannat@international.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.5.2 Project Authority *(to be inserted at contract award)*

The Project Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone: ___-___-_____
Facsimile: ___-___-_____
E-mail address: _____

In its absence, the Project Authority is:

Name: _____
Title: _____
Organization: _____
Address: _____

Telephone: ___-___-_____
Facsimile: ___-___-_____
E-mail address: _____

The Project Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

7.5.3 Contractor's Representative *(to be inserted at contract award)*

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: ___ ___ _____
E-mail address: _____

7.6 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.7 Payment

7.7.1 Basis of Payment

The Contractor will be paid for the Work performed, in accordance with the Basis of payment at annex “B”, to the limitation of expenditure specified. Customs duties are included and Applicable Taxes are extra.

7.7.2 Limitation of Expenditure

1. Canada's total liability to the Contractor under the Contract must not exceed $ _____. Customs duties are _____ (*insert "included", "excluded" or "subject to exemption"*) and Applicable Taxes are extra.
2. No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:
    a. when it is 75% committed, or
    b. four months before the contract expiry date, or
    c. as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work, whichever comes first.
3. If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

7.7.3 Method of Payment

Canada will pay the Contractor on a monthly basis for work performed covered by the invoice in accordance with the payment provisions of the Contract if:

a. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b. all such documents have been verified by Canada;

c. the Work performed has been accepted by Canada.

7.7.4 Electronic Payment of Invoices – Contract

The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

a. Direct Deposit

7.7.6 Discretionary Audit

The following are subject to government audit before or after payment is made:

a. The amount claimed under the Contract, as computed in accordance with the Basis of Payment, including time charged.
b. The accuracy of the Contractor's time recording system.
c. The estimated amount of profit in any firm-priced element, firm time rate, firm overhead rate, or firm salary multiplier, for which the Contractor has provided the appropriate certification. The purpose of the audit is to determine whether the actual profit earned on a single contract if only one exists, or the aggregate of actual profit earned by the Contractor on a series of negotiated contracts containing one or more of the prices, time rates or multipliers mentioned above, during a particular period selected, is reasonable and justifiable based on the estimated amount of profit included in earlier price or rate certification(s).
d. Any firm-priced element, firm time rate, firm overhead rate, or firm salary multiplier for which the Contractor has provided a "most favoured customer" certification. The purpose of such audit is to determine whether the Contractor has charged anyone else, including the Contractor's most favored customer, lower prices, rates or multipliers, for like quality and quantity of goods or services.

Any payments made pending completion of the audit must be regarded as interim payments only and must be adjusted to the extent necessary to reflect the results of the said audit. If there has been any overpayment, the Contractor must repay Canada the amount found to be in excess.

7.7.7 Time Verification

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

7.8 Invoicing Instructions

The Contractor must submit invoices in accordance with the following instructions. Invoices cannot be submitted until all work identified in the invoice is completed.

Each invoice must specify the following:

a. Company name, address, etc.;
b. Client address;
c. Date of the invoice;
d. Contract Number;
e. Total dollar amount;

Applicable Taxes must be calculated on the total amount of the invoice.

Invoices must be distributed as follows:

- One (1) copy must be forwarded to the Project Authority identified under the section entitled "Authorities" of the Contract.

7.9 Certifications and Additional Information

7.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

7.9.2 Federal Contractors Program for Employment Equity - Default by the Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.10 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

7.11 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

(a) the Articles of Agreement;
(b) the supplemental general conditions 4003 (2010-08-16), Supplemental General Conditions - Licensed Software. 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software.;
(c) the general conditions 2035 (2020-05-28), General Conditions - Higher Complexity – Services;
(d) Annex A, Statement of Work;
(e) Annex B, Basis of Payment;
(f) Annex C, Security Requirements Check List
(g) the Contractor's bid dated _____,

7.12 Foreign Nationals (Canadian Contractor *OR* Foreign Contractor)

SACC Manual clause A2000C _____ *(insert date)* Foreign Nationals (Canadian Contractor)

OR

SACC Manual clause A2001C _____ *(insert date)* Foreign Nationals (Foreign Contractor)

7.13 Insurance Requirements

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

7.14 Limitation of Liability

7.14.1 First Party Liability:

(a) **Contract Performance:** The Contractor is fully liable for all damages to Canada, arising from the Contractor's performance or failure to perform the Contract.

(b) **Data Breach**: The Contractor is fully liable for all damages to Canada resulting from its breach of security or confidentiality obligations resulting in unauthorized access to or unauthorized disclosure of records or data or information owned by Canada or a third party.

(c) **Limitation Per Incident:** Subject to the following section, irrespective of the basis or the nature of the claim, the Contractor's total liability per incident will not exceed the cumulative value of the Contract invoices for 12 months preceding the incident.

(d) **No Limitation**: The above limitation of Contractor liability does not apply to:

(i) willful misconduct or deliberate acts of wrongdoing, and

(ii) any breach of warranty obligations.

7.14.2 Third Party Liability: Regardless whether the third party claims against Canada, the Contractor or both, each Party agrees that it will accept full liability for damages that it causes to the third party in connection with the Contract. The apportionment of liability will be the amount set out by agreement of the Parties or determined by a court. The Parties agree to reimburse each other for any payment to a third party in respect of damages caused by the other, the other Party agrees to promptly reimburse for its share of the liability.

7.15 Safeguarding Electronic Media

a. Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.
b. If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.16 Dispute Resolution

(a) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.

(b) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.

(c) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.

(d) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

ANNEX A

STATEMENT OF WORK

1. Title

Hosted Web Based Application Solution for Foreign Affairs, Trade and Development Canada.

2. Background

Department of Foreign Affairs, Trade and Development Canada (DFATD) has a requirement for a Hosted Web Based Application Solution (HWBA) for the Europe, Middle East and African, the United States, the Asia Pacific and the Americas regions, consisting of ± 178 geographic locations who will require access but who will be serviced through seven (7) Common Service Delivery Points (CSDP). DFATD could establish more CSDP, open more diplomatic missions and/or proceed with some reorganizations either operational and/or geographical. HWBA shall be capable of accommodating any growth or reorganizations in our network.

3. Objective

The Department requires an HWBA solution to manage a high volume of applicants for advertised vacancies in various locations across the world. With CSDP Human Resources (HR) teams directing and coordinating all of the recruitment activity in the various locations, a new and improved system is required. The system must be an all-encompassing HR hiring platform designed to incorporate every hiring steps from posting vacancies, sourcing candidates to managing resume, administering exams, allowing online interviews and reference verification. The system must integrate and be compatible with the current versions, and all future commercially available versions, of at least, but not limited to Google Chrome, Microsoft Internet Explorer, Edge and Firefox, ensuring that the recruitment policy of the Department and the security policy of the Government of Canada are adhered to.

4. Scope

The HWBA is to cover a rigid recruitment process with strict criteria to be followed by all CSDP with options for add-ons approved by the departmental project authority and system Administrators. The contractor will work closely with the client to develop, adjust, configure and suggest improvements to the HWBA at the initial stage and when the system goes live.

The HWBA must include anything required to enable the Users to perform all of its features, meet this Statement of Work and provide the functionality as proposed by the contractor in its bid response. This includes, but is not limited to, providing any and all hosted software, access licenses, drivers, application programming interfaces (API), adapters, connectors and plug-ins.

5. Tasks/Specifications

a. The contactor must ensure that the work is done to the agreed standard of services.
b. The contractor must notify the Project Authority of critical issues and updates that may affect the required standard of services.
c. The contractor is liable for any and all damages incurred whether direct or indirectly through negligence.
d. The contractor is responsible for ensuring that its personnel follow the security and safety standards established by the contract authority.
e. The contractor must comply with all local and national regulations, practices and policies.

5.1 Mandatory requirements

All mandatory requirements **Attachment 1 Of Part 4**
and Point Rated criteria can be found in **Attachment 1 of Part 4**

5.2 Technical Specifications

The following technical specifications must be embedded within the HWBA:

1. All features of the HWBA should be available in Canadian English and Canadian French.
2. The HWBA must have the same look and feel as the corporate site (https://www.canada.ca/en.html).
3. An online testing environment and an online training environment must mirror the production environment. The working data in the testing environment and the training environment must be entirely artificial and must not contain any candidate and/or transaction data from the production environment.
4. A staging environment must be available to verify all releases prior to the move to production. The staging environment must never contain any candidate and/or transaction data from production.
5. A staging environment summary (RSS) feed for vacancies must be suitable for integration with other internet sites.
6. The production environment of the HWBA must be capable of handling the following estimated volumes:
    a. Ongoing access for up to 500 DFATD user accounts;
    b. Advertising up to 1000 vacancies per annum;
    c. Capturing and managing approximately 300,000 applications per annum; and
    d. The number of candidate applications and vacancies held in the system is to be unlimited.
7. The HWBA must integrate with the HR data base system currently used by the Government of Canada built using the Oracle PeopleSoft application. For this to happen, the Project Authority will provide all necessary access and/or data to the service provider.
8. The HWBA must be able to have all names and addresses of Canadian Embassy, High Commissions, Consulates and offices as required for communications with capability to update as may be required. A full list in Canadian English and Canadian French will be provided by the client as and when required.
9. The HWBA must feature a career opportunities section which must have search capabilities for candidates to search vacancies.
10. The HWBA must have multiple sections within the application interface process for candidates, which may include, but not limited to; terms and conditions for the candidate to agree to, standard sifting questions for the candidate to answer, a pre-agreed upon form where the candidate provides their experience, education and other predetermined information and the ability to upload a maximum of 3 documents no larger than 5 MB total.
11. The HWBA must allow candidates to edit their application while the competition remains open.

12. The HWBA must have a vacancy progress page for the client users to view vacancies which includes, but not limited to, the vacancy job title, location, classification, closing date and number of applications.

13. Competitions must automatically close at the date and time specified taking into account different time zones around the globe and a further option for the client to extend closing dates.

14. The HWBA must have a controlled recruitment process to track candidates through the process from start to finish limiting actions of the candidate as shown in the predefined workflow.

15. The HWBA must have a capacity to communicate with candidates with a predetermined automated communication via email, with standard templates in both Canadian English and Canadian French at specified stages of the process. Examples of these stages are, but not limited to; when the candidate first submits their application, whenever (within the process) they are vetted out, when they are invited to an assessment or interview, when they fail either an assessment or an interview, when they have passed all stages, when they have been identified as successful or when an outage is affecting the system's operations.

16. The HWBA must have assessment and interview modules available with self-booking slots for candidates. The client must be able to edit these slots during the process.

17. The HWBA must have the ability to have a talent pool of qualified candidates identified in a list specific to each competition.

18. The HWBA must have the ability to record basic letter of offer data templates for each location within each CSDP, which can be completed by the client, and forwarded as an attachment in an email or as a document to a system user or recipient outside of the system.

19. The HWBA must provide the facility to send standard template forms to client users for completion and return to the CSDP. Examples of this include job poster template and letter of offer.

20. The HWBA must offer a fully customizable vetting process for candidate applications in order to help vet out candidates who do not have specified qualifications. This process must include, but not be limited to:

    a. A question on the applicants' right to work in the country where the staffing process applies;
    b. Series of yes/no sifting questions for the candidate to answer; and
    c. Vetting out functions that shall reject applications that do not provide the required response.

21. The HWBA must have the option to send ad-hoc communication at a specified time for a group of or individual candidate communications.

22. The HWBA must have the option for standard time delays on specific communication emails sent to candidates.

23. The HWBA must have an automated reminder communication sent to candidates if they have not booked a slot prior to the assessment and/or interview scheduled date.

24. The HWBA must have the ability to print, share and/or download candidate documents in order to share easily with someone outside of the system.

25. The HWBA must have the capability to upgrade and/or customize the interface in order to meet the client's needs as and when discussed and agreed with the contractor.

26. The HWBA musts provide statistical (management) information, e.g. the average, median or mean time it took from one stage of the recruitment process to another such as the exam to interview stage for a series of categories such as by competition, by launch and closing date, by type or by level, etc.

27. The HWBA must have user customizable management information reporting abilities including, but not limited to, end of campaign, conversion, data mining (export to Microsoft Office Suite documents e.g. Excel), time to hire, reports regarding applicants as well as data reports on transactions by client users.

28. The HWBA must have audit capabilities.

29. The HWBA must record an audit history trail of all activity (i.e. actions and communications), which can be easily accessed (but not altered) by the client users.

30. The HWBA must offer different user access rights and views to the client. Examples of this would include a user account profile for CSDP HR staff, Hiring Managers and one for Administrators with specified override abilities. Administrator account option for override by CSDP HR personnel and HR departmental leads.

31. The HWBA must provide the client with the ability to manage the access to accounts (being able at a minimum to create, edit, delete and set expiration dates on user accounts). CSDP HR users should be able to create and edit Hiring Manager accounts and Super users should be able to create and edit CSDP HR users accounts.

32. The HWBA must have the option to send a notification to an identified approving manager when a user account has been set up in the system and/or other identified actions within the system.

33. The HWBA must ensure that access to the system by users includes a two-factor authentication process.

34. The HWBA must be maintained and upgraded throughout the entire contract period.

35. The HWBA must be available 24/7 – 365 days per year with an allowance for maintenance (no more than five (5) hours downtime in a standard week).

36. The contractor must respond to support technical tickets within 72 hours.

37. The HWBA must have a back-up system in place in the event there are any system failures. Data must not be lost due to any outages or failures. In the event of a system failure, administrators, users and applicants shall receive instant error message while full functions shall resume within 12 hours. Information saved prior to the outage shall be accessible to users and applicants with no data loss once the system is back on.

38. The HWBA must have capability for back end system upgrade and incremental features without disrupting the systems functions and the client's operations.

39. The HWBA must have maintenance functions i.e. corrective, preventative, adaptive and perfective maintenances.

40. The HWBA must work with current versions, and all future commercially available versions, of at least, but not limited to Google Chrome, Microsoft Internet Explorer, Edge and Firefox.

5.3 Training

Once the contract is awarded and the solution is in place, the contractor must provide training on the system on an “as and when requested” basis. The contractor must train approximately up to 100 designated client users so that they become familiar with the product and are able to use their training knowledge to perform their duties efficiently.

5.3.1 Scope of Training

The training must include all aspects of the system abilities necessary to access the system, use and administer it. All training sessions must have direct access to the contractor’s online training environment. The training course and material must cover all the information necessary to permit Authenticated client users to perform all tasks and responsibilities pertaining to their profiles.

5.3.2 Training Format

Training is required to be delivered both on-site (classroom) and/or remotely (i.e. Instructor-led training via web conference or web teleconference) in Canadian English and Canadian French for up to 6 training session in each official language. There will be separate training sessions for each of these languages. Trainers provided by the contractor will need to be fluent in the language of the requested training session.

The contractor must deliver the training documentation in Canadian English and Canadian French. If the training documentation is only available in Canadian English, it must be translated by the contractor to Canadian French within 80 days of contract award.

Before providing any training sessions, at least five (5) working days in advance of the first training session, the contractor must submit the course syllabus and schedule, the training materials, and the names and qualifications of the instructors to the Project Authority for approval.

5.3.3 Online Training Materials

The online training material and course must be hosted by the contractor and be available to view 24/7 days a week. The training material must remain current with the Production version and be updated prior to the deployment of the new functionality to the Production Environment.

The online training environment must mirror the production environment. However, the working data should be entirely artificial.

The online material must cover all aspects of the system including all updates to the training manuals at no charge. These online training manuals must be:

a. usable and available using the system throughout the Contract period;
b. printable by all pages, specific chapter, and by specific page range; and
c. available from the Production and Training environments.

6. Deliverables

After 30 calendar days of the contract being awarded, the contractor will provide a simple to use, safe and secure HWBA testing environment for CSDPs to recruit Locally Engaged Staff by advertising job vacancies via a careers opportunity website.

Within 24 hours after, contractor, client and DFATD IT experts will collaborate in assessing the testing environment, its customized functions and its security. Once deemed safe and fulsome by the project lead and IT experts, the contractor will finalize the solution for its formal launch and use.
Job vacancies hosted on the careers opportunity website will be accessed through links situated on DFATD Organization Web sites and various other Job poster sites (as an iframe). A “vacancy to hire” applicant tracking system will be provided by the contractor to map the recruitment process. The proposed system will cope with all categories of recruitment required by the client.

Once the contract will be awarded, the services must be provided in accordance with the mandatory requirements shown in **Attachment 1 of Part 4**. The contractor must provide adequate staffing levels required to fulfill the work resulting from the contract being awarded, as well as appropriate personnel, supervision and training.

The contractor will provide technical support for client users online and by telephone available 24/7-365 days per year. The contractor must also provide a form of technical support for candidates using the system. This includes assisting them with password resets. The contractor must define the technical support service and what options are being provided for both including the turnaround time for support.

7. Roles and responsibilities

The assigned Project Managers shall be responsible for project planning, design, development, testing and deployment. Project Managers will also be responsible for project and quality assurances, resolving system failures, managing all changes and customizations, resolving conflicting requirements. As users/candidates contact the contractor’s call center for support, project managers shall resolve issues being escalated to them internally. Project managers shall also suggest new security features as they become available.

8. Reporting and Communications

At no additional cost to DFATD, the contractor must interact with the Project Authority to provide regular and periodic updates on the progress made in the performance of the contractual obligations, as well as discuss and submit written reports on issues around the implementation and operational phases of the platform. Meetings will occur on an ad hoc basis and as problems arise. They will be coordinated by the Project Authority with a notice to the contractor at a minimum of three (3) working days ahead of meeting date and time. Nevertheless, the notice period could be shorter depending on the urgency of the matters.

9. Location of Work and Travel

Travel costs incurred while executing this contract will not be reimbursed nor paid separately. Therefore, the contractor is required to include travel costs in the service costing.

10. Language of Work

The official communication language should be English. The contractor must be able to communicate with Project Authority in Canadian English and Canadian French. Throughout the contract period, the contractor must provide e-mail support in Canadian English and Canadian French with qualified personnel and a web support portal that includes, as a minimum, frequently asked questions and on-line support tools, as approved by the client.

11. Security Requirements

In addition to the security requirements stated in **Attachment 1 of Part 4,** the Contractor must automatically monitor on a continuous basis events in order to:

a. detect attacks, Incidents and abnormal events against HWBA;
b. identify unauthorized use and access of HWBA Data and components, and.
c. respond, contain, and recover from threats and attacks against HWBA.

ANNEX B

BASIS OF PAYMENT

The Contractor must provide a firm all-inclusive rate for all work to be performed which includes cost of labour, direct materials and supplies, equipment, fringe benefits, general and administrative expenses, participant evaluations, overhead and profit and any other expenses that may be incurred for the contract.

All overhead expenses normally incurred in providing the services such as project office space and furnishings, word processing, work estimates, photocopying, courier and telephone charges, local travel are included in the firm rates identified hereunder and will not be permitted as direct charges.

Travel and Living Expenses will not be paid for any part of this contract including any relocation required to satisfy the terms of the contract.

The volumetric data specified below are provided for bid evaluated price determination purposes only. They are not to be considered as a contractual guarantee. Their inclusion in this pricing schedule does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

A- Initial Contract Period

Table – Initial Period (January 11th, 2021 to January 10th, 2024)				
Item No.	**Product**	**Quantity**	**Unit Price**	**Total Cost**
1	**Hosted Web Based Application Solution**			$0.00
2	***(Contractor, insert if applicable…)***			$0.00
			Total:	$0.00

B- Option Periods

Table – Option Period 01 (January 11, 2024 to January 10, 2025)				
Item No.	**Product**	**Quantity**	**Unit Price**	**Total Cost**
1	**Hosted Web Based Application Solution**			$0.00
2	**(Contractor, insert if applicable…)**			$0.00
			Total:	$0.00

Table – Option Period 02 (January 11, 2025 to January 10, 2026)				
Item No.	**Product**	**Quantity**	**Unit Price**	**Total Cost**
1	**Hosted Web Based Application Solution**			$0.00
2	**(Contractor, insert if applicable…)**			$0.00
			Total:	$0.00

Table – Option Period 03 (January 11, 2026 to January 10, 2027)				
Item No.	**Product**	**Quantity**	**Unit Price**	**Total Cost**
1	**Hosted Web Based Application Solution**			$0.00
2	**(Contractor, insert if applicable…)**			$0.00
			Total:	$0.00

Table – Option Period 04 (January 11, 2027 to January 10, 2028)				
Item No.	**Product**	**Quantity**	**Unit Price**	**Total Cost**
1	**Hosted Web Based Application Solution**			$0.00
2	**(Contractor, insert if applicable…)**			$0.00
			Total:	$0.00

Applicable taxes extra (GST + QST)

Auto-Renewal Opt Out. Canada hereby provides notice to the Contractor that it opts out of any auto-renewal of the term obligation. The Contractor acknowledges receipt of the notice, and represents that this Contract will be valid only until the end of the Contract Period, as defined above.

C- Total Estimated Contract Value for Evaluation Purpose

Evaluated Price (total cost initial contract period + total cost of all option periods)**: $** _____

ANNEX C SECURITY REQUIREMENTS CHECK LIST

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: 20-160060

Security Classification / Classification de sécurité: unclassified

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Global Affairs Canada
2. Branch or Directorate / Direction générale ou Direction: AES
3. a) Subcontract Number / Numéro du contrat de sous-traitance
3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work / Brève description du travail: Hosted Web based Application Solution
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées? No / Non: X — Yes / Oui:
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? No / Non: X — Yes / Oui:
6. Indicate the type of access required / Indiquer le type d'accès requis
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) No / Non: — Yes / Oui: X
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. No / Non: X — Yes / Oui:
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit? No / Non: X — Yes / Oui:
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada: X	NATO / OTAN:	Foreign / Étranger:

7. b) Release restrictions / Restrictions relatives à la diffusion

Canada	NATO / OTAN	Foreign / Étranger
No release restrictions / Aucune restriction relative à la diffusion: X	All NATO countries / Tous les pays de l'OTAN:	No release restrictions / Aucune restriction relative à la diffusion:
Not releasable / À ne pas diffuser:		
Restricted to: / Limité à :	Restricted to: / Limité à :	Restricted to: / Limité à :
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

Canada	NATO	Foreign / Étranger
PROTECTED A / PROTÉGÉ A: X	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ:	PROTECTED A / PROTÉGÉ A:
PROTECTED B / PROTÉGÉ B:	NATO RESTRICTED / NATO DIFFUSION RESTREINTE:	PROTECTED B / PROTÉGÉ B:
PROTECTED C / PROTÉGÉ C:	NATO CONFIDENTIAL / NATO CONFIDENTIEL:	PROTECTED C / PROTÉGÉ C:
CONFIDENTIAL / CONFIDENTIEL:	NATO SECRET / NATO SECRET:	CONFIDENTIAL / CONFIDENTIEL:
SECRET / SECRET:	COSMIC TOP SECRET / COSMIC TRÈS SECRET:	SECRET / SECRET:
TOP SECRET / TRÈS SECRET:		TOP SECRET / TRÈS SECRET:
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT):		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT):

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité: unclassified

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
~~TBC~~ 20-160060

Security Classification / Classification de sécurité
unclassified

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No / Non [x] Yes / Oui [ ]
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No / Non [x] Yes / Oui [ ]
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

[x] RELIABILITY STATUS / COTE DE FIABILITÉ	[ ] CONFIDENTIAL / CONFIDENTIEL	[ ] SECRET / SECRET	[ ] TOP SECRET / TRÈS SECRET
[ ] TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	[ ] NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ] NATO SECRET / NATO SECRET	[ ] COSMIC TOP SECRET / COSMIC TRÈS SECRET
[ ] SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : contractor shall obtain a RS clearance. Contractor to clear his/her own staff involved in contract being awarded (criminal backgrounds checks, debts checks, enhanced reference checks, etc)

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No / Non [X] Yes / Oui [ ]
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non [x] Yes / Oui [ ]
Dans l'affirmative, le personnel en question sera-t-il escorté?
NOT APPLICABLE AS CONTRACTOR WILL DELIVER SERVICE IN HIS OWN PREMISES

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No / Non [ ] Yes / Oui [X]
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No / Non [X] Yes / Oui [ ]
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No / Non [X] Yes / Oui [ ]
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No / Non [ ] Yes / Oui [X]
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No / Non [x] Yes / Oui [ ]
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada | Gouvernement du Canada

Contract Number / Numéro du contrat
~~TBS~~ 20-160060

Security Classification / Classification de sécurité
unclassified

PART C - (continued) / PARTIE C - (suite)

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens	X															
Production																
IT Media / Support TI	X															
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

☒ No / Non ☐ Yes / Oui

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

☒ No / Non ☐ Yes / Oui

Government of Canada | Gouvernement du Canada

Contract Number / Numéro du contrat
20-160060

Security Classification / Classification de sécurité
unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	Date
FELICIA ZEVGOLIS	DEPUTY DIRECTOR, AFS	Felicia Zevgolis	July 17, 2019

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel
203-1811		felicia.zevgolis@international.gc.ca

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	Date
Hussen Mussa	A/ Security in Contracting	Hussen Mussa	2020-01-30

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel
343-203-3080		hussen.mussa@international.gc.ca

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? / Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?
[X] No / Non [ ] Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	Date
Brendan Hua/SPP	Sr Specialist, Supply ops		July 17, 2019

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel
203-1307		brandon.hua@international.gc.ca

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print)	Title - Titre	Signature	Date
Anik Farrell - CSO 613-946-5194 anik.farrell@tpsgc-pwgsc.gc.ca		Farrell, Anik Digitally signed by Farrell, Anik Date: 2020.02.04 10:01:12 -05'00'	

Telephone	télécopieur	E-mail address - Adresse courriel

ATTACHEMENT 3.1 OF THE BID SOLICITATION

BID SUBMISSION FORM

BID SUBMISSION FORM		
Bidder's full legal name		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Bidder's Procurement Business Number (PBN) [see the Standard Instructions 2003] **[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]**		
Jurisdiction of Contract: Province or territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Former Public Servants See the Article in Part 2 of the bid solicitation entitled Former Public Servant for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
	Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
Security Clearance Level of Bidder		

[include both the level and the date it was granted] **[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]**		
On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that: 1. The Bidder considers itself and its proposed resources able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.		
Signature of Authorized Representative of Bidder		

ATTACHMENT 1 OF PART 4

BID EVALUATION CRITERIA

Mandatory Technical Criteria

The bid must meet the mandatory technical criteria specified below. The Bidder must provide the necessary documentation to support compliance with this requirement.

Bids which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

The proposal will be evaluated and scored in accordance with specific evaluation criteria as detailed herein. It is imperative that these criteria be addressed in sufficient depth in the proposal to fully describe the bidder's response.

Bidders are advised that only listing experience without providing any supporting data to describe responsibilities, duties and relevance to the requirements will not be considered "demonstrated" for the purpose of this evaluation and will be deemed non-compliant. Cutting and pasting the experience into the resumes will not suffice.

The bidder should provide complete details as to where, when (month and year) and how (through which activities/responsibilities) the stated qualifications/experience were obtained. Experience gained during formal education shall not be considered work experience. All requirements for work experience shall be obtained in a legitimate work environment as opposed to an educational setting. Co-op terms are considered work experience as they are related to the required services.

Bidders are also advised that the month(s) of experience listed for a project whose timeframe overlaps that of another referenced project will only be counted once. For example: Project 1 timeframe is July 2001 to December 2001; Project 2 timeframe is October 2001 to January 2002; the total months of experience for these two projects references is seven (7) months. Bidders are asked to indicate on the resumes how many months/years are to be counted for each project. **Each project must be a minimum of three (3) months in duration to be considered.**

Merely stating the experience is not sufficient and the proposal will be deemed non-compliant unless demonstrated.

For each criterion, details should be provided regarding the qualifications, relevant experience and expertise of the proposed personnel. For mandatory and point rated requirements, the experience of the proposed resource(s) must be clearly identified by providing a summary/description of the previous projects worked on and indicating when the work was carried out, and the client.

Curriculum vitae of the proposed resources must be provided. Also, the evaluation criteria matrix must be used to answer the mandatory criteria. Therefore, the answers are to be entered directly into the matrix, explaining how each criterion has been met, while referencing both the page and project numbers as indicated in the resume/CV.

The consensus evaluation team will consist of two (2) teams. One team will be responsible for the evaluation of the Business Requirements. The other team consisted of IM/IT Security experts will solely be responsible for the evaluation of the Security Requirements.

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
Business requirements		
M1	The bidder must provide a HWBA (Host Web Based Application) in accordance with the Annex A – Statement of Work, with the capability to integrate with a third-party candidate-testing tool for booking, scheduling and notification purposes. The system must integrate every hiring steps from posting vacancies, sourcing candidates to managing resume, administering exams, allowing online interviews and reference verification.	
M2	The bidder must propose two (2) Project Managers by submitting the resource's current resumes.	
M3	The bidder MUST demonstrate, using detailed project descriptions, that each of the proposed resources has a minimum of five (5) years of experience working as a Project Manager in designing, developing and integrating significant size and complexity software, program and/or application. *Significant size is defined as 500 users and managing 300 000 applications.	
M4	The bidder MUST demonstrate using detailed project descriptions, that the bidder has experience in providing HWBA systems to large organizations*. *Large organizations defined as a minimum of 1000 employees.	
M5	The bidder MUST demonstrate using detailed project descriptions, that the bidder has experience in developing and fully implementing the proposed system on an international scale.	
Security requirements		
M6 **Roles and responsibilities for Security**	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Solution between the Supplier (any Supplier Sub-processors, as applicable) and Canada. In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (a) Account management; (b) Boundary protection; (c) Asset and information system backup; (d) Incident management; (e) System monitoring; and (f) Vulnerability management.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
M7 **Data Protection**	The physical locations of the Commercially Available Public Software as a Service (which may contain Canada's data) and define in the must be located in either: (a) A country within the North Atlantic Treaty Organization (NATO). Additional information on countries within NATO can be located at the following link: https://www.nato.int/cps/en/natohq/nato_countries.htm ; (b) A country within the European Union (EU). Additional information on countries within the EU can be located at the following link: https://europa.eu/european-union/about-eu/countries_en; or (c) A country with which Canada has an international bilateral industrial security instrument. The Contract Security Program has international bilateral industrial security instruments with the countries listed on the following PSPC website: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html#s9 and as updated from time to time. The Supplier must provide documentation that demonstrates how the proposed Commercially Available Public Software as a Service submitted meets the mandatory requirement outlined in Data Protection Requirements. To be considered compliant, the provided documentation must include: (a) An up-to-date list of the physical locations (including city and country) for each data centre that may contain Canada's data including in backups or for redundancy purposes. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M8 **Data Center Facilities**	The Supplier of the proposed Commercially Available Public Software as a Service must implement security measures that ensure the protection of IT facilities and information system assets on which GC data (up to protected A information) is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	This includes, at a minimum: (a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; (b) proper handling of IT media; (c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; (d) controlled access to information system output devices to prevent unauthorized access to Canada's data (up to protected A information); (e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; (f) escorting visitors and monitoring visitor activity; (g) maintaining audit logs of physical access; (h) controlling and managing physical access devices; (i) enforcing safeguarding measures for GC data (up to protected A information) at alternate work sites (e.g., telework sites); and (j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data (up to protected A information) using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms. The Supplier must provide documentation that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: (a) system documentation or technical documentation outlining and detailing the security measures including policies, process and procedures that are used to grant and maintain the required level of security screening for the Software as a Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M9 **Personnel Security**	The Supplier of the proposed Commercially Available Public Software as a Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data (for up to Protected A information) is stored and processed. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: (a) description of the employee and subcontractor positions that require access to Canada's Data (for up to Protected A information) or have the ability to affect the confidentiality, integrity or availability of the Services; (b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; (c) process for security awareness and training as part of employment onboarding and when employee and subcontractor roles change; (d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and (e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or on the reliability of Software as a Services hosting GC assets and data (for up to Protected A information). The Supplier must provide documentation that demonstrates how the Software as a Service Provider of the proposed Commercially	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	Available Public Software as a Service complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: (a) system documentation or technical documentation outlining and detailing the security measures including policies, process and procedures that are used to grant and maintain the required level of security screening for the Software as a Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data (for up to Protected A information) is stored and processed. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M10 **Third Party Assurance**	The Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing information security policies, procedures, and security controls. For suppliers that have already completed the security assessment by providing to CCCS their certifications and audit reports and have already entered into a Non-Disclosure Agreement (NDA) with them, must send their certifications and audit reports directly to CCCS client services at contact@cyber.gc.ca in order to meet this requirement. For suppliers that have not completed the security assessment, the onboarding process will commence once the Submission complies with the requirements of the Request for Supply Arrangements, meets all mandatory technical and financial evaluation criteria, and provides all of the mandatory certifications in order to be declared responsive. PSPC will then refer the Supplier to CCCS client services to begin the onboarding process to the IT Assessment and to enter into an NDA with them in order to receive a copy of the onboarding submission form and any additional information required to meet this requirement. The Supplier must provide documentation that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. The Supplier must provide the following industry certifications for the proposed Service to demonstrate compliance: (a) European Union General Data Protection Regulation (GDPR); And one of the following: i. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or ii. AICPA Service Organization Control (SOC) 2 Type II (b) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. Each provided certification and assessment report must: 1. Be valid as of the Submission date; 2. Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP; 3. Identify the current certification date and/or status; 4. identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. 5. The scope of the report must map to locations and services offered by the proposed Supplier. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and 6. Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality management system standard. **Please note:** • Certifications must be provided for all portions of the proposed Service identified; • Certifications must be accompanied by assessment reports; and Certifications must be valid and within the 12 months prior to the start of a contract.	
M11 **Supply Chain Management**	The Supplier must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, including Cloud Service Providers, etc.) that would provide Canada with the proposed Commercially Available Public Software as a Service.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	For the purposes of this requirement, a company who is merely a supplier of goods to the Software as a Service Provider of the proposed Commercially Available Public Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Public Software as a Services of the Software as a Service Provider that have been proposed by the Supplier. **Please note**: Suppliers are advised that subsequent procurement Streams may require the Supplier to notify Canada regularly when there are updates to the list of third party suppliers. The Supplier must provide documentation list of Sub processors that could be used to perform any part of the Services in providing Canada with the Services. The list must include the following information (i) the name of the Sub processor; (ii) the identification of the scope activities that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the activities required to support the Services. For SaaS, the Contractor must demonstrate that the IaaS/PaaS leveraged by the Services: (a) Supplier Sub-processors have been assessed by the CCCS Program as per; and (b) Supplier meet the security obligations for Sub-Processors and/or Subcontractors outlined by the Supplier, for the life of the contract. If the Supplier of the proposed Commercially Available Public Software as a Service does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, the Supplier is requested to indicate this in their response to this requirement.	
M12 **Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Public Software as a Service must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within the supply chain. The Supplier must demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in Supply Chain Risk Management Requirements as documented under the Software as a Service Provider Information Technology Security Assessment	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	program. To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Software as a Service Provider's approach to SCRM and demonstrate how the Supplier of the proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks.	
M13 **Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrate how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services; (b) Restrict and minimize access to the Services and Canada's Data's to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Canada's Data's; (d) Constrain all access to service interfaces that host Assets and Canada's Data's to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions)	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	(https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; (h) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets; (j) Access controls on objects in storage and granular authorization policies to allow or limit access; (k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel. The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: (a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The documentation, cannot simply be a repetition of the mandatory requirement but must explain and demonstrate and indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers., on how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M14 **Federation of Identity**	Federation of Identity The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and (c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service system administrator user account(s). The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. To be considered compliant, the provided documentation must include: (a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or enduser documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
M15 **Endpoint Protection**	The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. To be considered compliant, the provided documentation must include: (a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M16 **Secure Development**	The Supplier must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. To be considered compliant, the provided documentation must include:	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	(a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M17 **Supplier Remote management**	The Supplier must manage and monitor remote administration of the Supplier's Service that are used to host GC services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points; (d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; (e) Authorize remote execution of privileged commands and remote access to security relevant information. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. To be considered compliant, the provided documentation must include: (a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Supplier Remote Management.	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M18 **Information Spillage**	1. The Supplier must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific data elements that is involved in a System's contamination; (b) A process to isolate and eradicate a contaminated System; and (c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination; (d) The supplier will confirm a point of contact, proper procedures and an agreed upon secure form of communication to provide assistance where practicable for customer administrators. 2. Upon request of Canada, the Supplier must provide a document that describes the Supplier's Information Spillage Response Process. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. To be considered compliant, the provided documentation must include: (a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage. The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M19 **Cryptographic Protection**	The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic -algorithms-unclassified-protected-andprotected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://cyber.gc.ca/en/cryptographic-module-validation-program-cmvp), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and; (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection. To be considered compliant, the provided documentation must include:	

Number	Mandatory Criteria	Cross Reference to Proposal *[supplier to insert]*
	(a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection The documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.	
M20 **Data Segregation**	The Supplier must implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and; (b) The separation of customer resources in multitenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another. The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.	

Point Rated Technical Criteria

Proposals will be evaluated and scored in accordance with specific evaluation criteria as detailed in this section. A bidder must obtain a minimum pass mark of **70% (45 out of 65)** in order to be considered responsive. Details should be provided regarding the qualifications, relevant experience and expertise of the proposed personnel. The experience of the proposed resource should be clearly identified by providing a summary/description of the previous projects worked on and indicating when the work was carried out, and the client.

Bidders are advised that only listing experience without providing any supporting data to describe responsibilities, duties and relevance to the requirements will not be considered “demonstrated” for the purpose of this evaluation. The bidder should provide complete details as to where, when (month and year) and how (through which activities/responsibilities) the stated qualifications/experience were obtained. Experience gained during formal education shall not be considered work experience. All requirements for work experience shall be obtained in a legitimate work environment as opposed to an educational setting. Co-op terms are considered work experience provided they are related to the required services.

Bidders are also advised that the month(s) of experience listed for a project whose timeframe overlaps that of another referenced project will only be counted once. **For example**, Project 1 timeframe is July 2001 to December 2001; Project 2 timeframe is October 2001 to January 2002; the total months of experience for these two project references is seven (7) months.

It is requested that for each of the criteria, bidder statements in this section make direct reference, project identifier, page number, to the supporting section(s) in the proposed resource's resume.

Number	Point Rated Technical Criteria	Cross Reference to Proposal *[Supplier to Insert]*	Point Allocation	Max Available Points	Points Received
R1	The Bidder should provide a detailed transition plan explaining how new system will go live. The transition plan should: • Identify steps involved in transferring historic data into the new system. • Identify how old system data will co-exist along with new data. Old data should be accessible for reporting functions and compiled along with new data for hiring processes occurring under the old system/new system; • Include the methodology for ensuring the timely delivery of work.		**Poor** – Vaguely described and/or not particularly clear; incomplete understanding of the requirement (**0 pt**) **Fair** – Some detail provided but still weak; some understanding of the transition associated with the requirement (**5 pts**) **Adequate** – Expanded description; conveys a basic understanding of the transition (**10 pts)** **Good** – Conveys a clear understanding of the transition but some detail missing with regards to old data usage (**15 pts**) **Excellent** – Meets the requirements of the SOW; all concerns addressed thoroughly and transition is properly envisioned (**20 pts**)	20	

Number	Point Rated Technical Criteria	Cross Reference to Proposal *[Supplier to Insert]*	Point Allocation	Max Available Points	Points Received
R2	The bidder should demonstrate, using detailed project descriptions, that each of the proposed project managers have experience working as a Project Manager in designing, developing and integrating significant size and complexity software, program and/or application.		Less than 5 years **(0 pt)** 5 to 9 years **(5 pts)** 10 years and more **(10 pts)** Both resources must meet the criteria in order to receive the full points.	10	
R3	The bidder should demonstrate that the proposed project managers each hold a valid* post-secondary degree. A copy of the certification must be submitted with the bid for points to be allocated. *Valid certification is defined as any degree from IT, computer sciences or engineering or any other relevant field from a recognized Canadian post-secondary institution.		College or CEGEP degree / IT Academy or Institute degree **(2 pts)** University degree **(5 pts)** Both resources must meet the criteria in order to receive the full points.	5	
R4	The bidder should demonstrate using detailed project descriptions, that the bidder has experience in providing HWBA systems to large organizations*. *Large organizations defined as a minimum of 1000 employees.		**5 pts** per organization	15	
R5	The bidder should demonstrate using detailed project descriptions, that the firm has experience in developing and fully implementing the proposed system on an international scale.		1 to 2 project **(5 pts)** 3 to 4 projects **(10 pts)** 5 projects and more **(15 pts)**	15	
Total			***Minimum pass mark (70% = 45 pts)***	**65**	**/65**

ATTACHMENT 1 TO PART 5 OF THE BID SOLICITATION

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the Employment Equity Act.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)